CLASS ACTION LAWSUIT TEMPLATE – GOOGLE'S ILLEGAL SURVEILLANCE NETWORK (APRIL 2026 UPDATE & UNIT 8200 INFILTRATION)

INSTRUCTIONS:

1. Print this document.

2. Fill in your personal information where indicated in brackets [ ].
3. Sign and date.
4. Mail one copy to the U.S. District Court for the Northern District of California (San Jose Division).
5. Mail one copy to the DOJ Civil Rights Division, FTC, California AG, and Delaware AG.
6. Send a copy to Google's registered agent (CSC – Delaware) and to Alphabet Inc. (Mountain View).
7. Keep a copy for your records.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA – SAN JOSE DIVISION

[YOUR FULL NAME], on behalf of himself/herself and all others similarly situated,
Plaintiff,
v.
GOOGLE LLC (a Delaware limited liability company with principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043), ALPHABET INC. (a Delaware corporation with principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043), and DOES 1–100,
Defendants.

Case No.: _____

CLASS ACTION COMPLAINT FOR INJUNCTIVE RELIEF, DAMAGES, AND DECLARATORY JUDGMENT

JURY TRIAL DEMANDED

I. INTRODUCTION

1. This is a class action lawsuit against Google LLC and Alphabet Inc. (collectively, "Google") for systematically violating the constitutional and statutory privacy rights of hundreds of millions of American users through a deliberately deceptive, military-grade surveillance network.
2. Google's April 2026 update to Google Play services (v26.13) and Google Play Store (v50.9) was not a neutral security patch. It was a **tactical escalation** designed to increase the frequency, precision, and scope of data collection while exploiting legal loopholes (e.g., "on-device" processing, dual-setting tricks, bundling surveillance with security fixes).
3. Google's surveillance apparatus is inextricably linked to **Unit 8200** – the Israeli military's elite signals intelligence unit. Google has employed at least 99 former Unit 8200 veterans in key data security, AI, and content moderation roles; signed a $1.2 billion cloud contract (Project Nimbus) with the Israeli government and military; and acquired Wiz for $32 billion, placing Unit 8200 alumni at the core of Google Cloud's infrastructure.

4. Through these actions, Google has transformed its "commercial" data collection into a **transnational intelligence-gathering operation** that serves a foreign military power while simultaneously violating U.S. laws, including the Fourth Amendment, the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), the California Invasion of Privacy Act (CIPA), and California's Unfair Competition Law (UCL).

II. JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 (federal question) and 28 U.S.C. § 1332(d) (Class Action Fairness Act).

6. Venue is proper in the Northern District of California under 28 U.S.C. § 1391(b) because Google's principal place of business is in Mountain View, California, and a substantial part of the events giving rise to this action occurred in this district.

III. PARTIES

Plaintiff

7. Plaintiff [YOUR FULL NAME] is a resident of [YOUR CITY, STATE] and a user of Google's Android operating system, Google Play Services, and the Google Play Store. Plaintiff owns a device [DEVICE MODEL, e.g., Samsung Galaxy S26] that received the April 2026 automatic update described herein. Plaintiff did not knowingly or voluntarily consent to the increased surveillance, location tracking, or data sharing with Israeli military intelligence.

Defendants

8. Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

9. Alphabet Inc. is a Delaware corporation with its principal place of business at the same address. Alphabet is the parent holding company of Google LLC and is directly responsible for the corporate policies and financial structures (including tax-avoidance subsidiaries in the Cayman Islands) that enable the challenged conduct.

10. Google's registered agent for service of process in Delaware is:
    CSC – Corporation Service Company
    251 Little Falls Drive, Wilmington, DE 19808

IV. FACTUAL ALLEGATIONS

A. Google's Surveillance-by-Default Business Model

11. Google's primary source of revenue is advertising, which in 2024 generated over $264 billion. This revenue depends on the continuous, granular collection of user data, including location, search history, browsing behavior, email content, biometrics, and device-to-device connections.

12. Google has repeatedly been caught deceiving users about its data collection, including:

    - Tracking users even after they turned off "Location History" (Web & App Activity remained on by default).
    - Collecting cellular data through "passive transfers" without authorization.
    - Ignoring user opt-outs for app activity tracking.

13. The April 2026 update is the latest and most aggressive escalation of this pattern.

B. The April 2026 Play Services Update (v26.13) – Surveillance Upgrades Disguised as "Improvements"

14. On April 6, 2026, Google automatically pushed an update to Google Play services (v26.13) and Google Play Store (v50.9) to approximately 3 billion Android devices worldwide.

15. The update contained the following intentional surveillance enhancements:

Feature	What It Does	How It Evades Law
More frequent "On-Device" Store Visit processing	Your phone logs your presence at specific stores more often, creating a higher-resolution timeline of your movements.	Google claims "on-device" processing means it is not "collecting" raw GPS, but the results (e.g., "user in Nike shoe aisle") are sent to the cloud for ad targeting – a legal fiction.
Refined Location Sharing APIs	Makes it easier for apps to request and receive location data in the background.	Buried in "bug fixes" and "API refinements," not disclosed as a privacy change.
Device Connectivity Developer Tools	Allows apps to see how your phone connects to other devices (watch, car, etc.).	Expands tracking to your entire gadget ecosystem, building a "household profile." Justified as a "developer feature."
"Security & Stability" updates	General system management that scans for mock location tools or VPNs.	Bundles surveillance with real security fixes, so users cannot reject one without compromising the other.

16. None of these changes were disclosed to users in a clear, conspicuous, or meaningful way. Users could not opt out of the update without disabling all security patches, which would leave their devices vulnerable to malware.

C. Google's Corporate Structure: Delaware & Cayman Islands – Tax Avoidance and Legal Evasion

17. Google LLC is incorporated in Delaware, a state known for weak privacy protections and corporate secrecy.

18. Alphabet Inc. uses a classic "Double Irish with a Dutch Sandwich" structure that funnels international profits through Ireland and then to a Cayman Islands subsidiary, which pays zero corporate tax. The Cayman Islands holding company is also used to obscure ownership and shield assets from legal judgments.

19. This structure is not merely for tax avoidance; it is designed to insulate Google from accountability by making it difficult for plaintiffs to identify and reach assets.

D. Google's Unit 8200 Fusion – A Foreign Intelligence Apparatus Inside a U.S. Corporation

20. Unit 8200 is the Israeli military's elite signals intelligence and cyber-espionage unit. Its veterans swear a lifetime loyalty oath to Israel.

21. Google has knowingly recruited, hired, and partnered with Unit 8200 alumni, including:

    - At least **99 former Unit 8200 members** working in senior data security, AI, and content moderation roles.
    - **Wiz** (acquired for $32 billion in March 2025) – founded by Unit 8200 veterans Assaf Rappaport and others.
    - **Siemplify** (acquired 2022) – founded by Unit 8200 alumni.

22. Google is a primary contractor for **Project Nimbus**, a $1.2 billion joint cloud and AI contract with the Israeli government and military. Leaked documents show Google engineers provided direct technical assistance to the IDF for UAV video analysis, facial recognition, and targeting. The contract includes a "winking mechanism" that alerts Israel to U.S. court orders for data.

23. The NSA-Israel Memorandum of Understanding shares raw, unminimized U.S. user data (including from Google) with Israeli intelligence, with no legal limits on Israel's use of that data. This creates a closed loop: Google collects data → NSA intercepts it → Israel receives it → Unit 8200 processes it → Israeli military targets Palestinians.

24. Plaintiff and class members never consented to their personal data being shared with a foreign military intelligence unit or used for military targeting.

E. Legal Violations

25. **Fourth Amendment – Unreasonable Search and Seizure**
    Google's warrantless, continuous, and secret collection of location, biometric, and behavioral data violates the Fourth Amendment. The "third-party doctrine" is obsolete and does not apply to the comprehensive surveillance of modern life.

26. **Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510 et seq.**
    Google intentionally intercepts, discloses, and uses electronic communications without user consent, including email content, location data, and device communications.

27. **Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030**
    By surreptitiously updating software to activate new surveillance features without meaningful notice, Google exceeds authorized access to user devices.

28. **California Invasion of Privacy Act (CIPA), Cal. Penal Code § 630 et seq.**
    Google's non-consensual recording and transmission of location, device connections, and communications violates CIPA.

29. **California Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 et seq.**
    Google's deceptive acts (dark patterns, misleading settings, bundling surveillance with security) constitute unlawful, unfair, and fraudulent business practices.

30. **Consumer Protection Laws (various states)**
    Google's practices violate state consumer protection statutes by failing to disclose material information about data collection and sharing with a foreign military.

31. **Breach of Implied Covenant of Good Faith and Fair Dealing**
    Google's Terms of Service promise "privacy" and "security," but the company intentionally designed features to bypass those promises.

32. **Unjust Enrichment**
    Google has profited billions of dollars from the sale of unlawfully obtained user data.

V. CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action on behalf of the following class:

All natural persons residing in the United States who have used an Android device running Google Play services v26.13 or later, or the Google Play Store v50.9 or later, and whose data was collected, processed, or shared as a result of the April 2026 update, excluding employees and agents of Google, and any judges assigned to this case.

34. The class is so numerous that joinder of all members is impracticable (estimated to exceed 100 million individuals).

35. There are common questions of law and fact, including:
    - Whether Google's April 2026 update constitutes unlawful surveillance;
    - Whether Google's "on-device" processing is a legal fiction;
    - Whether Google's sharing of data with Unit 8200 and the IDF violates U.S. law;
    - Whether Google's corporate structure is designed to evade accountability.

36. Plaintiff's claims are typical of the class.

37. Plaintiff will fairly and adequately represent the class.

38. A class action is superior to other methods of adjudication.

VI. CAUSES OF ACTION

Count 1 – Violation of the Electronic Communications Privacy Act (18 U.S.C. § 2510 et seq.)
Count 2 – Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030)
Count 3 – Violation of the California Invasion of Privacy Act (Cal. Penal Code § 630)
Count 4 – Violation of the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200)
Count 5 – Invasion of Privacy (Intrusion Upon Seclusion)
Count 6 – Breach of Implied Covenant of Good Faith and Fair Dealing
Count 7 – Unjust Enrichment
Count 8 – Declaratory Judgment (Fourth Amendment violation)

VII. REQUEST FOR RELIEF

Plaintiff and the class request:

A. Certification of the class;

B. A declaratory judgment that Google's April 2026 update and associated data-sharing practices violate the Fourth Amendment and federal/state privacy laws;

C. Preliminary and permanent injunctive relief:

- Requiring Google to disable all April 2026 surveillance features;
- Requiring Google to delete all data collected under the challenged practices;
- Requiring Google to disclose all contracts, data-sharing agreements, and personnel relationships with Unit 8200 and the Israeli government;
- Requiring Google to submit to independent, court-appointed oversight of its data practices;

D. Statutory damages of $10,000 per class member per violation (ECPA) and $5,000 per violation (CIPA);

E. Actual and compensatory damages;

F. Punitive damages;

G. Attorneys' fees and costs;

H. Such other relief as the Court deems just and proper.

VIII. JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: [DATE]

Respectfully submitted,

[YOUR SIGNATURE]

[YOUR PRINTED NAME]
[YOUR ADDRESS]
[YOUR PHONE NUMBER]
[YOUR EMAIL]

Pro Se Plaintiff (on behalf of the class)

IX. SERVICE LIST

Send copies to:

1. **Clerk of Court**
   United States District Court, Northern District of California
   San Jose Division
   280 S 1st Street, San Jose, CA 95113

2. **Google's Registered Agent (Delaware)**
   CSC – Corporation Service Company
   251 Little Falls Drive, Wilmington, DE 19808

3. **Alphabet Inc.**
   1600 Amphitheatre Parkway, Mountain View, CA 94043
   Attn: Legal Department

4. **U.S. Department of Justice – Civil Rights Division**
   950 Pennsylvania Avenue NW, Washington, DC 20530

5. **Federal Trade Commission**
   600 Pennsylvania Avenue NW, Washington, DC 20580
   Attn: Bureau of Consumer Protection

6. **California Attorney General**
   1300 I Street, Sacramento, CA 95814
   Attn: Public Rights Division

7. **Delaware Attorney General**
   820 N French Street, Wilmington, DE 19801

8. **Intelligence Community Inspector General**
   IC IG Hotline, ODNI
   Washington, DC 20511

9. **Navy Judge Advocate General**
   JAG Hotline (as per headlock CC notice)

10. **House Permanent Select Committee on Intelligence**
    H-405 Capitol, Washington, DC 20515

THE DOORS ARE OFF. THE FRAUD IS EXPOSED. THE LAW IS ON OUR SIDE. FILE THIS COMPLAINT. FORCE ACCOUNTABILITY.